Guia de Segurança do Netra Modular System

Número do Item: E68387-01
Agosto de 2015

Número do Item: E68387-01

Copyright © 2015, Oracle e/ou suas empresas afiliadas. Todos os direitos reservados e de titularidade da Oracle Corporation. Proibida a reprodução total ou parcial.

Este programa de computador e sua documentação são fornecidos sob um contrato de licença que contém restrições sobre seu uso e divulgação, sendo também protegidos pela legislação de propriedade intelectual. Exceto em situações expressamente permitidas no contrato de licença ou por lei, não é permitido usar, reproduzir, traduzir, divulgar, modificar, licenciar, transmitir, distribuir, expor, executar, publicar ou exibir qualquer parte deste programa de computador e de sua documentação, de qualquer forma ou através de qualquer meio. Não é permitida a engenharia reversa, a desmontagem ou a descompilação deste programa de computador, exceto se exigido por lei para obter interoperabilidade.

As informações contidas neste documento estão sujeitas a alteração sem aviso prévio. A Oracle Corporation não garante que tais informações estejam isentas de erros. Se você encontrar algum erro, por favor, nos envie uma descrição de tal problema por escrito.

Se este programa de computador, ou sua documentação, for entregue / distribuído(a) ao Governo dos Estados Unidos ou a qualquer outra parte que licencie os Programas em nome daquele Governo, a seguinte nota será aplicável:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Este programa de computador foi desenvolvido para uso em diversas aplicações de gerenciamento de informações. Ele não foi desenvolvido nem projetado para uso em aplicações inerentemente perigosas, incluindo aquelas que possam criar risco de lesões físicas. Se utilizar este programa em aplicações perigosas, você será responsável por tomar todas e quaisquer medidas apropriadas em termos de segurança, backup e redundância para garantir o uso seguro de tais programas de computador. A Oracle Corporation e suas afiliadas se isentam de qualquer responsabilidade por quaisquer danos causados pela utilização deste programa de computador em aplicações perigosas.

Oracle e Java são marcas comerciais registradas da Oracle Corporation e/ou de suas empresas afiliadas. Outros nomes podem ser marcas comerciais de seus respectivos proprietários.

Intel e Intel Xeon são marcadas comerciais ou marcas comerciais registradas da Intel Corporation. Todas as marcas comerciais SPARC são usadas sob licença e são marcas comerciais ou marcas comerciais registradas da SPARC International, Inc. AMD, Opteron, o logotipo da AMD e o logotipo do AMD Opteron são marcas comerciais ou marcas comerciais registradas da Advanced Micro Devices. UNIX é uma marca comercial registrada licenciada por meio do consórcio The Open Group.

Este programa ou equipamento e sua documentação podem oferecer acesso ou informações relativas a conteúdos, produtos e serviços de terceiros. A Oracle Corporation e suas empresas afiliadas não fornecem quaisquer garantias relacionadas a conteúdos, produtos e serviços de terceiros e estão isentas de quaisquer responsabilidades associadas a eles, a menos que isso tenha sido estabelecido entre você e a Oracle em um contrato vigente. A Oracle Corporation e suas empresas afiliadas não são responsáveis por quaisquer tipos de perdas, despesas ou danos incorridos em consequência do acesso ou da utilização de conteúdos, produtos ou serviços de terceiros, a menos que isso tenha sido estabelecido entre você e a Oracle em um contrato vigente.

Acessibilidade da Documentação

Para obter informações sobre o compromisso da Oracle com a acessibilidade, visite o Web site do Programa de Acessibilidade da Oracle em `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Acceso ao Oracle Support

Os clientes da Oracle que adquiriram serviços de suporte têm acesso a suporte eletrônico por meio do My Oracle Support. Para obter informações, visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` caso tenha deficiência de audição.

Conteúdo

Visão Geral da Segurança

O Oracle Netra Modular System é uma plataforma pré-integrada e pré-cabeada que pode ser totalmente virtualizada para reduzir custos e tempo de implantação no seu centro de dados. O sistema modular inclui o hardware que você especificou e é montado na fábrica e enviado para você.

Esses tópicos descrevem conceitos de segurança e recursos do sistema modular:

Princípios Básicos de Segurança

Siga esses princípios básicos de segurança para todos os componentes de software e hardware do sistema modular:

- Autenticação - Consiste no modo como um usuário é identificado, normalmente por meio de informações confidenciais, como nome de usuário e senha, ou chaves compartilhadas. A autenticação consiste em garantir que os usuários do hardware ou software são quem eles dizem ser. Por padrão, senhas e nomes de usuários locais são usados para autenticação. A autenticação baseada em chaves compartilhadas também está disponível.
- Contabilidade e Auditoria - Referem-se à manutenção de um registro das atividades do usuário no sistema. Os recursos de software e hardware do sistema modular permitem que os administradores monitorem atividades de logon e mantenham inventários de hardware:
  - Os log-ins de usuários são monitorados por meio de logs do sistema. O administrador do sistema e as contas de serviços têm acesso a comandos que, se usados de maneira incorreta, poderiam causar danos e perdas de dados.
  - Os ativos de hardware são controlados por meio de números de série. Os números de peça da Oracle são gravados eletronicamente em cartões, módulos e placas-mãe e podem ser usados para fins de inventário.

Considerações Avançadas sobre Segurança

Além dos princípios básicos de segurança, o sistema modular cuida da capacidade de sobrevivência e da defesa em profundidade. O sistema modular fornece um conjunto bem integrado de recursos de segurança para atender aos requisitos e preocupações de segurança. As seções a seguir descrevem esses princípios:

- Capacidade de Sobrevivência de Cargas de Trabalho de Missão Crítica – As organizações que escolhem as plataformas de hardware e software para cargas de trabalho de missão crítica podem ter a certeza de que o sistema modular pode evitar ou minimizar o dano causado por ações acidentais e maliciosas tomadas por usuários internos e externos. Como parte das melhores práticas da Oracle Maximum Availability Architecture, as práticas a seguir podem aumentar a capacidade de sobrevivência:
  - Garantir que os componentes usados sejam projetados, desenvolvidos e testados para funcionarem juntos em suporte às arquiteturas de implantação segura. O sistema modular suporta o isolamento seguro, o controle de acesso, a qualidade de serviço e o gerenciamento seguro.
  - Reduzir a superfície de ataque padrão dos componentes ajuda a diminuir a exposição total da máquina.
  - Proteger a máquina, inclusive as interfaces operacionais e de gerenciamento, usando um complemento de protocolos abertos e verificados, bem como APIs capazes de suportar metas de segurança tradicionais de autenticação forte, controle de acesso, confidencialidade, integridade e disponibilidade.
  - Verificar se o software e o hardware contêm recursos que mantêm o serviço disponível quando ocorre uma falha. Esses recursos ajudam nos casos em que os invasores tentam desativar um ou mais componentes individuais no sistema.
- Defesa em Profundidade para Proteger o Ambiente Operacional – O sistema modular emprega vários controles de segurança independentes e que contribuem uns com os outros para ajudar a criar um ambiente operacional seguro para dados e cargas de dados. O sistema modular suporta o princípio de defesa em profundidade da seguinte maneira:
  - Oferecendo um forte complemento de mecanismos de defesa para proteger informações em trânsito, em uso e em inércia. Os controles de segurança estão disponíveis no servidor e nas camadas de rede. Controles de segurança exclusivos de cada camada podem ser integrados aos outros para permitir a criação de arquiteturas de segurança fortes e em camadas.
  - Suportando o uso de padrões abertos e bem definidos, protocolos e interfaces. O sistema modular pode ser integrado a políticas de segurança, arquiteturas, práticas e padrões existentes.

Recursos de Segurança

O hardware e o software do sistema modular são fortalecidos. A Oracle também fornece configurações de segurança recomendadas para serviços como NTP e SSH. Além disso, a arquitetura do sistema modular fornece recursos de segurança para os principais componentes. Na maioria das vezes, esses recursos de segurança são aplicados por organizações que estão implantando uma estratégia de segurança em camadas. Os recursos são agrupados nas seguintes categorias:

Isolamento de Tráfego de Rede

Se você quiser consolidar a infraestrutura de TI, implementar arquiteturas de serviços e entregar serviços multilocatários seguros, considere o isolamento do tráfego de rede. O sistema modular fornece a flexibilidade para implementar as políticas de isolamento e estratégias com base em necessidades.

No nível da rede física, o acesso ao cliente é isolado com base no gerenciamento de dispositivos e da comunicação entre dispositivos. O tráfego de clientes e de gerenciamento de rede é isolado em redes separadas. O acesso ao cliente é fornecido por uma rede Ethernet redundante de 10 Gbps que garante um acesso confiável e de alta velocidade a serviços em execução no sistema. O acesso ao gerenciamento é fornecido por meio de uma rede Ethernet de 1 Gbps separada fisicamente. Isso fornece uma separação entre redes operacionais e de gerenciamento.

As organizações podem optar por segregar ainda mais o tráfego da rede por meio da rede Ethernet de acesso ao cliente configurando LANs virtuais (VLANs). As VLANs segregam o tráfego de rede com base em seus requisitos. A Oracle recomenda o uso de protocolos criptografados nas VLANs para assegurar a confidencialidade e a integridade das comunicações.

Oracle ILOM para Gerenciamento Seguro

Os conjuntos de recursos e controles de segurança são necessários para proteger devidamente aplicativos e serviços individuais. É igualmente importante ter recursos de gerenciamento abrangentes para manter a segurança dos sistemas e serviços implantados. O sistema modular usa os recursos de gerenciamento de serviços do Oracle ILOM.

O Oracle ILOM é um SP incorporado aos nós de computação do sistema modular. O Oracle ILOM é usado para executar atividades de gerenciamento fora da banda, como as seguintes:

- Fornecer acesso seguro para executar o gerenciamento seguro de luzes dos servidores de armazenamento e banco de dados. O acesso inclui acesso baseado na Web protegido por SSL, acesso à linha de comandos usando o Secure Shell e protocollos IPMI v2.0 e SNMPv3.
- Separar requisitos de tarefas usando o modelo de controle de acesso baseado em funções. São atribuídas funções específicas a usuários individuais que limitam as funções as quais podem ser executadas.
- Evitar um registro de auditoria de todos os logons e alterações de configuração. Cada entrada do log de auditoria lista o usuário que está executando a ação e um registro de data e hora. O registro de auditoria permite que as organizações detectem alterações ou atividades não autorizadas e atribua essas ações de volta a usuários específicos.

Para obter mais informações sobre a segurança do Oracle ILOM, consulte o *Oracle ILOM Security Guide* em `http://www.oracle.com/goto/ILOM/docs`.

Planejando um Ambiente Seguro

Aplique diretrizes de segurança antes de instalar o Netra Modular System. Depois que o sistema estiver instalado, revise e ajuste periodicamente as diretrizes de segurança para que estejam atualizadas em relação aos requisitos de segurança da sua organização.

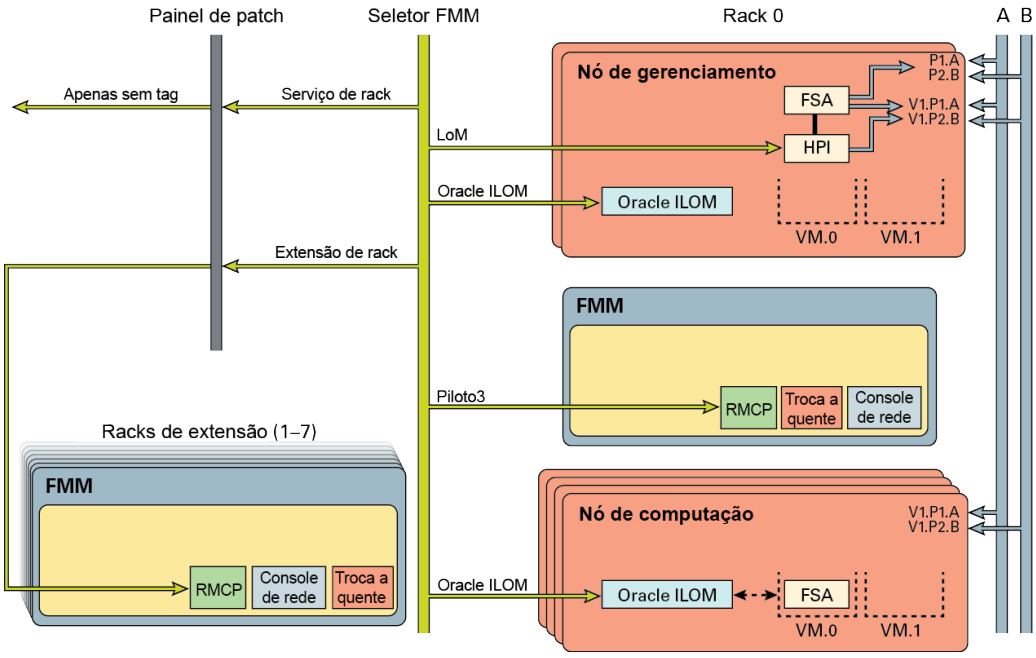
Esses tópicos fornecem diretrizes de segurança para a instalação do Netra Modular System:

Entre em contato com o Oficial de Segurança de TI para obter requisitos de segurança adicionais específicos para o seu sistema e ambiente.

Rede Padrão

A figura e as descrições a seguir explicam a rede padrão do Netra Modular System.

- O Sistema/Rede de Telemetria (rede de luz verde) inclui a porta LoM do nó de gerenciamento no VLAN 4090 por meio do seletor FMM.
- A Rede ILOM de Telemetria em um intervalo VLAN 4094 com FMM inclui o Oracle ILOM de nós de computação, bem como o Oracle ILOM por meio do FMM dos nós de rede.
- O painel de patch estende a Rede de Telemetria para racks de 1 a 7. Uma configuração com vários racks suporta as mesmas sub-redes e a mesma VLAN com um ID de rack diferente
- A VLAN(1) fornece outros serviços para a Rede de Telemetria por meio de uma autenticação adequada.
- As Redes de Dados (A &B) fornecem acesso em banda ao nó FSA.
- O aplicativo de HA pode gerenciar os racks por meio de interfaces expostas do sistema modular (JMX, C- API e assim por diante).



Contas de Usuário

Essa tabela lista os usuários e as senhas padrão dos componentes do sistema modular. Altere todas as senhas padrão depois de instalar o Netra Modular System.

Componente	Nome do Usuário e Senha
Switches Ethernet	`root/changeme` **Observação -** Proteja os valores `enable mode password` e `secret` do usuário `admin`.
Nós de computação e gerenciamento	`root/changeme`

Configurações de Segurança Padrão

O sistema modular é instalado com várias configurações de segurança padrão. Sempre que possível e prático, defina configurações padrão seguras. Consulte as configurações padrão na sua versão do Oracle ILOM em `http://www.oracle.com/goto/ILOM/docs`.

Protegendo o Hardware

O isolamento físico e o controle de acesso são a base em que você constrói a arquitetura de segurança. Garantir que o sistema físico esteja instalado em um ambiente seguro protege-o contra o acesso não autorizado. Da mesma forma, o registro de todos os números de série ajuda a evitar o uso não autorizado dos componentes de hardware.

Estas seções fornecem diretrizes gerais sobre segurança do hardware para o sistema modular.

Restrições de Acesso

- Instale os sistemas e o equipamento relacionado em um local trancado e com acesso restrito.
- Se o equipamento for instalado em um rack com uma porta com trava, só destranque a porta do rack durante a manutenção dos componentes no rack. O travamento das portas também restringe o acesso aos dispositivos hot-plug ou hot-swap.
- Guarde todas as peças de reposição sobressalentes em um gabinete que possa ser trancado. Restrinja o acesso ao gabinete bloqueado para a equipe autorizada.
- Periodicamente, verifique o status e a integridade das travas no rack e no gabinete de peças para protegê-los contra, ou detectar, falsificação ou portas destravadas acidentalmente.
- Guarde as chaves do gabinete em um local seguro com acesso limitado.
- Restrinja o acesso às consoles USB. Dispositivos como controladores de sistema, PDUs e seletores de rede podem ter conexões USB. O acesso físico é um método mais seguro de acessar um componente, já que ele não é suscetível a ataques baseados na rede.
- Conecte a console a um KVM externo para permitir o acesso remoto à console. Em geral, os dispositivos KVM suportam autenticação de dois fatores, controle de acesso centralizado e auditoria. Para obter mais informações sobre as diretrizes de segurança e as melhores práticas para KVMs, consulte a documentação que acompanha o dispositivo KVM.

Números de Série

Registre cuidadosamente todos os números de série quando os componentes forem recebidos e colocados no inventário. Isso impossibilita o uso de componentes de hardware não autorizados. Antes de qualquer componente ser instalado ou usado, confirme sua autenticidade comparando o respectivo número de série com o que foi registrado quando o componente foi recebido. Siga estas práticas para proteger o hardware:

- Mantenha um registro dos números de série de todos os componentes de hardware.
- Faça uma marca de segurança em todos os itens relevantes de hardware do computador, como peças de reposição. Use canetas especiais ultravioletas ou etiquetas em alto-relevo.
- Mantenha as chaves e licenças de ativação de hardware em um local seguro que esteja facilmente acessível para o gerente do sistema em emergências de segurança. Os documentos impressos talvez sejam o seu único comprovante de propriedade.

Os leitores de identificação por radiofrequência (RFID) sem fio podem simplificar ainda mais o rastreamento de ativo. Consulte a documentação da Oracle, *How to Track Your Oracle Sun System Assets by Using RFID*, em http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf.

Unidades de Disco Rígido

Discos rígidos são geralmente usados para armazenar informações confidenciais. Para proteger essas informações contra a divulgação não autorizada, esvazie as unidades de disco rígido antes de reutilizá-las, descontinuá-las ou descartá-las.

- Consulte as políticas de proteção de dados para determinar o método mais apropriado de limpeza das unidades de disco rígido.
- Se necessário, utilize o Serviço de Retenção de Dispositivos e de Dados do Cliente da Oracle.

  http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf

Protegendo o Software

A maior parte da segurança de hardware é implementada por meio de medidas de software. Estas seções fornecem diretrizes gerais de segurança de software do Netra Modular System.

Impedir o Acesso Não Autorizado (Oracle Linux)

- **Use os comandos do SO Linux para restringir o acesso ao software do Oracle Solaris, fortalecer o SO, usar recursos de segurança e proteger aplicativos.**

  Consulte *Oracle Linux Security Guide for Release 6* em `http://docs.oracle.com/cd/E37670_01/E36387/html/index.html`.

Impedir o Acesso Não Autorizado (Oracle ILOM)

- **Use os comandos do Oracle ILOM para restringir o acesso ao software do Oracle ILOM, alterar a senha definida de fábrica, limitar o uso da conta de superusuário root e proteger a rede privada para o SP.**

  Consulte a sua versão do *Oracle ILOM Security Guide* em `http://www.oracle.com/goto/ILOM/docs`.

Impedir o Acesso Não Autorizado (Oracle VM Server com o Oracle Linux)

- **Use os comandos do Oracle Linux para restringir o acesso ao software do Oracle VM Server, utilizar recursos de segurança e proteger aplicativos.**

  Consulte *Oracle VM Security Guide for Release 3.3* em `http://docs.oracle.com/cd/E50245_01/E50254/html/index.html`.

Segurança do Oracle Hardware Management Pack

O Oracle Hardware Management Pack apresenta dois componentes: um agente de monitoramento SNMP e uma família de ferramentas de interface da linha de comando do sistema operacional cruzado (CLI Tools) para gerenciamento do sistema.

- Plug-ins do Hardware Management Agent – o SNMP é um protocolo padrão que monitora ou gerencia um sistema. Com os Plug-ins SNMP do Hardware Management Agent, é possível usar o SNMP para monitorar sistemas Oracle no seu centro de dados com a vantagem de não precisar se conectar a dois pontos de gerenciamento: o host e o Oracle ILOM. Essa funcionalidade permite usar um único endereço IP (o endereço IP do host) para monitorar vários sistemas.

  Os plug-ins SNMP são executados no sistema operacional do host dos sistemas Oracle. O Plug-in SNMP estende o agente SNMP nativo no sistema operacional do host para fornecer outros recursos do Oracle MIB. O Oracle Hardware Management Pack não contém ele próprio um agente SNMP. Para o Oracle Linux, um módulo é adicionado ao agente `net-snmp`. Para o Microsoft Windows, o plug-in estende o serviço SNMP nativo. Todas as configurações de segurança relacionadas ao SNMP para o Oracle Hardware Management Pack são determinadas pelas configurações do agente ou serviço SNMP nativo, e não pelo plug-in.

  O SNMPv1 e o SNMPv2c não fornecem criptografia e usam strings de comunidade como uma forma de autenticação. O SNMPv3 é mais seguro e é a versão recomendada porque usa a criptografia para fornecer um canal seguro, além de nomes de usuário e senha individuais.
- Documentação do Oracle Hardware Management Pack – Para ver diretrizes de segurança que são específicas do Oracle Hardware Management Pack, consulte o *Oracle Hardware Management Pack (HMP) Security Guide* em `http://www.oracle.com/goto/OHMP/docs`.

Localizando Guias de Segurança Relacionados

Guias de Segurança

Esses guias descrevem políticas e procedimentos para manter seguros os produtos relacionados:

- *Oracle Server X5-2 Security Guide*
- *Oracle Switch ES2-72 and Oracle Switch ES2-64 Security Guide*
- *Oracle Linux Security Guide for Release 6* em `http://docs.oracle.com/cd/E37670_01/E36387/html/index.html`
- *Oracle ILOM Security Guide* em `http://www.oracle.com/goto/ILOM/docs`
- *Oracle VM Security Guide for Release 3.3* em `http://docs.oracle.com/cd/E50245_01/E50254/html/index.html`
- *Oracle Hardware Management Pack (HMP) Security Guide* em `http://www.oracle.com/goto/OHMP/docs`